said EAS device, said gate including said reader one of built integrally thereto and in a proximity thereof.

20. (Amended) The method according to claim 15, further comprising:

providing said computer with a database including information regarding said authorized user of said object; and

operatively coupling an alarm to said security path,

wherein upon passage through said path, said EAS device triggers the path to activate said alarm.

REMARKS

Claims 1-20 are all the claims presently pending in the application. Claim 7 stands rejected upon informalities (e.g., 35 U.S.C. § 112, second paragraph), and claims 1-8 and 10-20 stand rejected on prior art grounds.

Claim 9 has been amended in a manner believed fully responsive to all points raised by the Examiner. It is noted that the term "one of..." was used to avoid the term "or" and is believed fully acceptable by the U.S.P.T.O. However, to speed prosecution, the term "one of..." has been amended for the Examiner. Reconsideration and withdrawal of this rejection are respectfully requested.

With respect to the prior art rejections, claims 1, 4, 6-7, 12, 14-15, 18 and 20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Swartz, et al. (U.S. Patent No. 5,979,758) in view of Burger (U.S. Patent No. 6,219,439). Claims 2 and 16 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Swartz, et al., in view of Burger and further in view of Bacon (U.S. Patent No. 5,984,388). Claims 3 and 17 stand rejected under 35 U.S.C. §

103(a) as being unpatentable over Swartz, et al., in view of Burger and further in view of Dames, et al. (U.S. Patent No. 6,054,924). Claims 5, 8, and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Swartz, et al., in view of Burger and further in view of Belka, et al. (U.S. Patent No. 5,777,884). Claim 10 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Swartz, et al., in view of Burger and further in view of Davis, et al. (U.S. Patent No. 5,748,085). Claims 11 and 13 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Swartz, et al., in view of Burger.

These rejections are respectfully traversed in view of the following discussion.

Attached hereto is a marked-up version of the changes made to the claims by the current Amendment.

It is noted that the claim amendments herein are made only for more particularly pointing out the invention for the Examiner, and not for distinguishing the invention over the prior art, narrowing the claims, or for any statutory requirements of patentability.

I. THE CLAIMED INVENTION

Applicant's invention, as disclosed and claimed (e.g., see independent claim 1), is directed to a system (and method) for preventing theft of an object, which includes an electronic article surveillance (EAS) device operatively attached to an object, a security path for detection of the EAS device, a reader operatively coupled to the security path, and a smart card for being read by the reader. The smart card contains an identification profile of an authorized user of the object.

A key feature of the invention is that the excitation source, that would otherwise enable the EAS device (e.g., antitheft tag) to be operative at the gate, is turned off.

Independent claim 15 recites a somewhat similar method, but with some different limitations.

With such unique and unobvious features and aspects of the invention, fast, reliable tracking of personnel carrying objects (computers) into/out of an area can be achieved. Further, a legitimate user can easily disable an interrogation device upon the presentation of suitable credentials (e.g., a smart card or the like).

Additionally, such a method and system are much more convenient than having the object (e.g., a computer) disabled and then having to reenable the computer upon recovery or if a mistake has occurred.

That is, with the invention, the disabling function is part of the interrogation path (e.g., gate). Thus, only the gate need be disabled and then subsequently reenabled, as opposed to the object (e.g., computer) itself. This disabling/reenabling of the gate significantly simplifies the antitheft problem. This is in complete contrast to the cited references such as Swartz, Burger, etc.

Such features are not taught or suggested by any other prior art of record, either alone or in combination.

II. THE PRIOR ART REJECTIONS

A. The § 103 Rejection based on Swartz in view of Burger

Applicant respectfully disagrees with the Examiner's reasoning and position. Indeed, the claimed invention differs substantially from the Examiner's cited prior art.

Swartz discloses a self-checkout point of transaction system including deactivatable electro-optically coded surveillance tags. Burger discloses a biometric authentication system.

First, there would have been no reason or motivation to combine the references in the manner urged, absent hindsight reconstruction of Applicant's invention based on nothing more

than a thorough reading of Applicant's own specification. Indeed, each of Swartz and Burger address completely different problems and it comes as no surprise that each offers a completely different structure for addressing such disparate problems.

That is, the self checkout POT system of Swartz for use with deactivatable coded surveillance tags has nothing to do with the biometric authentication system of Burger, let alone attempting to achieve fast, reliable tracking of personnel carrying objects (computers) into/out of an area, or of allowing a legitimate user to easily disable an interrogation device upon the presentation of suitable credentials, as in the claimed invention.

Thus, the Examiner's rejection(s) fail on this ground alone.

Secondly, even assuming arguendo that the references would have been combined, the claimed invention would still not have been produced.

That is, a key difference between the claimed invention and the cited art to Swartz in view of Burger is that the claimed invention turns off the excitation source that would otherwise enable the EAS device (e.g., antitheft tag) to be operative at the gate.

(2)

More specifically, the present invention does nothing to disable the tag as Swartz does. As a result (and as mentioned above), the inventive tag never needs to be reprogrammed or reset for future use since it is never changed. Instead, only the excitation source is "changed".

In contrast, Swartz et al. optically scans the antitheft tag or the bar code thereon which then sends information to a data base from which a decision is made to deactivate the tag. This is far different from the claimed invention. Indeed, nowhere does optical scanning of the anti-theft tag occur in the present application. Thus, Swartz et al. fails to "change" the excitation source (e.g., fails to turn off the excitation source that would otherwise enable the antitheft tag to be operative at the interrogation path).

This is an important difference between the claimed invention and Swartz et al. and Burger, as well as the other cited references.

Thus, there is no teaching or suggestion of "a computer attached to said reader, said computer disabling a security gate if a person entering said security path is authorized to remove said object", as defined in independent claims 1 and 15. Indeed, Swartz et al. teaches away from this by disabling the tag, not the security gate. Burger does nothing to mitigate this teaching away by Swartz et al.

In sum, none of the cited art deactivates the alarm system (e.g., the security gate).

Again, with respect to Bacon, Dames, Davis, Belka et al., etc. nothing is added by their disclosures that make up for the deficiencies of Swartz et al. in view of Burger.

Finally, Applicant respectfully disagrees with the Examiner description regarding the operation of an acoustomagnetic tag. Such tags do not emit acoustic waves.

Instead, this type of tag, typically manufactured, for example, by Sensormatic Inc., refers to the acousto-magnetic effect in which an amorphous magnetic thin sample, biased by a small hard magnet within the tag resonates mechanically due to its longitudinal dimension and elastic coupling. As a result, a magnetic wave is output at a frequency equal to the frequency of the excitation magnetic field. Then, the excitation field is turned off and the ring down signal from the tag is read by the detection system as long as the tag has not been disabled. Disabling or deactivation occurs by changing the bias field within the tag.

Thus, in complete and fundamental contrast with the Examiner's urged combination of prior art references, the claimed invention includes key limitations not in any way taught or suggested by the cited references. Additionally, none of the other applied references, either alone or in combination, makes up for the deficiencies of Swartz in view of Burger.

Turning to the claim language, there is no teaching or suggestion of independent claim 1

which recites "*[a] system for preventing theft of an object, comprising:*

an electronic article surveillance (EAS) device operatively attached to an object;

a security path for detection of said EAS device;

a reader operatively coupled to said security path; [and]

a smart card for being read by said reader, said smart card containing an identification profile of an authorized user of said object; and

a computer attached to said reader, said computer disabling a security gate if a person entering said security path is authorized to remove said object (emphasis Applicant's), as defined by independent claim 1.

Further, there is no teaching or suggestion of independent claim 15 which recites "*[a] method for preventing theft of an object, comprising:*

operatively attaching an electronic article surveillance (EAS) device to an object;

detecting said EAS device as said object traverses a security path;

operatively coupling a reader to said security path;

reading, by said reader, a smart card being presented to said reader as said object traverses said security path, said smart card containing an identification profile of an authorized user of said object; and

attaching a computer to said reader, said computer disabling a security gate if a person entering said security path is authorized to remove said object (emphasis Applicant's).

For all of the reasons stated above, the claimed invention is fully patentable over the cited references.

Further, the other cited prior art of record has been reviewed, but it too even in combination with the applied references, fails to teach or suggest the claimed invention.

III. FORMAL MATTERS AND CONCLUSION

Applicant notes the PTO-948 form attached to the Office Action and directed to the drawings originally filed with the application on May 7, 1999. However, formal drawings were filed on June 22, 1999. Accordingly, Applicant respectfully request approval and acknowledgment of receipt of the formal drawings filed on June 22, 1999.

In view of the foregoing, Applicant submits that claims 1-20, all the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: 6/21/02

Sean M. McGinn, Esq.
Reg. No. 34,386

McGinn & Gibb, PLLC
8321 Old Courthouse Rd. Suite 200
Vienna, VA 22182-3817
(703) 761-4100
Customer No. 21254

VERSION SHOWING MARKINGS MADE

IN THE CLAIMS:

1. (Amended) A system for preventing theft of an object, comprising:

an electronic article surveillance (EAS) device operatively attached to an object;

a security path for detection of said EAS device;

a reader operatively coupled to said security path; [and]

a smart card for being read by said reader, said smart card containing an identification profile of an authorized user of said object; and

a computer attached to said reader, said computer disabling a security gate if a person entering said security path is authorized to remove said object.

5. (Amended) The system according to claim 1, wherein said [security path includes a] gate is for interrogating said EAS device, said gate including said reader one of built integrally thereto and in a proximity thereof.

6. (Amended) The system according to claim 1, [further comprising a computer coupled to said reader,] wherein said computer [containing] contains a database including information regarding said authorized user of said object.

9. (Amended) The system according to claim 7, wherein [one of] either said alarm is turned off [and] or an authorized user is allowed free passage through said path, when said authorized person exhibits said smart card to said reader.

15. (Amended) A method for preventing theft of an object, comprising:

operatively attaching an electronic article surveillance (EAS) device to an object;

detecting said EAS device as said object traverses a security path;

operatively coupling a reader to said security path; [and]

reading, by said reader, a smart card being presented to said reader as said object traverses said security path, said smart card containing an identification profile of an authorized user of said object; and

attaching a computer to said reader, said computer disabling a security gate if a person entering said security path is authorized to remove said object.

19. (Amended) The method according to claim 15, wherein said security [path includes a] gate is for interrogating said EAS device, said gate including said reader one of built integrally thereto and in a proximity thereof.

20. (Amended) The method according to claim 15, further comprising:

[coupling a computer to said reader,] providing said computer [containing] with a database including information regarding said authorized user of said object; and

operatively coupling an alarm to said security path,

wherein upon passage through said path, said EAS device triggers the path to activate said alarm.